

AFFIDAVIT OF MATTHEW K. O'NEILL

I, Matthew K. O'Neill, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since 1998. I received formal training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, and the United States Secret Service Academy in Beltsville, Maryland. I am currently assigned to the United States Secret Service, Manchester Resident Office. My current assignment includes investigating violations of Title 18, United States Code, Sections 1028, 1028A, 1029, 1030, 1341, 1343, 1344 and 1956 on the internet. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.
2. As set forth herein, the USSS is currently investigating an unknown individual who claimed to be the CEO of Besi, a company based in Europe, with a Salem, New Hampshire subsidiary. This unknown individual, through telephone and email communications, convinced the Salem subsidiary's controller to send approximately \$2.6 million dollars via wire transfers to banks located in Asia, all in violation of 18 U.S.C. §§ 1343 (wire fraud) and 1344 (bank fraud).
3. I am submitting this affidavit in support of an Application for a Search Warrant to search records and other information (including the contents of communications) associated with a certain account, specifically **max.ring@lawyer.com**, that is stored at premises owned, maintained, controlled, or operated by 1&1 Mail & Media ("1&1 Mail"), an e-mail provider headquartered at 701 Lee Road, Suite 300, Chesterbrook, PA 19087. The information to be searched is described in the following paragraphs and in Attachment A.
4. Based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1343 & 1344 have been committed by these and other unknown targets/suspects. There is also probable cause to believe that records and other information associated with e-mail accounts **max.ring@lawyer.com** as described in Attachment A, contain evidence, fruits, and/or instrumentalities of various violations of Title 18, United States Code, Sections 1343 & 1344, as detailed and specified herein below. Accordingly, there is probable cause to search the information described in Attachment A for evidence, fruits, and/or instrumentalities of these crimes, as described in Attachment B. This affidavit is made in support of an Application for a Search Warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to compel 1&1 Mail, a provider of electronic communication and remote computing services, to provide certain items as set forth in Attachment B, Part I, hereto, and for the government to search and to seize certain items as set forth in Attachment B, Part II, hereto.

5. The facts set forth in this affidavit are based upon my personal observations, my review of documents and computer records, my training and experience, and information obtained from other agents and witnesses, including from other law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge of the investigation into this matter.

II. PROBABLE CAUSE

6. Your affiant believes that there is probable cause to believe that violations of Title 18, United States Code, Sections 1343 & 1344 have been committed by these and other targets and that evidence, instrumentalities, and/or fruits of criminal activity will be found in a search of computer servers hosted at 1&1 Mail, for the following reasons.
7. In or about December 2013, I became aware that Besi, a global company with headquarters in Duiven, the Netherlands, was defrauded out of approximately \$2.6 million dollars. This fraud occurred when an unknown individual posed as Besi's CEO, Richard Blickman.
8. This unknown individual contacted Besi's Salem subsidiary on November 25, 2013 and spoke to the Salem subsidiary's controller, David Egan. The unknown individual spoke with a Dutch accent and claimed to be Besi CEO, Richard Blickman. During this call with Egan, the unknown individual said "This is Richard, I am working on an investment in China and it is strictly confidential. This must stay between you, my lawyer and myself until the deal is done. What is your current cash position?" Egan told the unknown individual that the Salem subsidiary had "approximately 2 million" on hand. In response, the unknown individual said, "This is what I would like you to do, wire 796k EU. I will have my lawyer send you an invoice that must be sent in EUR. Here is his e-mail address. (The unknown individual provided max.ring@lawyer.com.) Please use Max's email when corresponding and he will contact me to stay updated." The unidentified individual also stated that he hoped to have the transfer completed by the end of the week.
9. From November 25, 2013 thru December 11, 2013, Egan had daily email correspondence with the max.ring@lawyer.com account. For example, on November 25, 2013, someone from the max.ring@lawyer.com account sent Egan an email that contained an attachment, which was an invoice for 796,000 EU and contained bank account information for Hong Kong where Egan was supposed to wire the funds. During the course of this fraud scheme, Egan and the max.ring@lawyer.com account exchanged numerous emails that included additional invoices and confirmations that funds were wired.
10. Based on my review of the records and other evidence obtained to date in this investigation, I believe that there is probable cause that the suspect e-mail account contain fruits, instrumentalities or evidence of the wire and bank fraud scheme.

III. TECHNICAL BACKGROUND

11. In my training and experience, I have learned that 1&1 Mail provides a variety of on-line services, including electronic mail ("e-mail") access to the general public. 1&1 Mail allows subscribers to obtain e-mail accounts at the domain name 1&1 Mail.com, like the e-mail account, **max.ring@lawyer.com**, listed in Attachment A. Subscribers obtain an account by registering with 1&1 Mail. During the registration process, 1&1 Mail asks subscribers to provide basic personal information. Therefore, the computers of 1&1 Mail are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for 1&1 Mail subscribers) and information concerning subscribers and their use of 1&1 Mail services, such as account access information, e-mail transaction information, and account application information.
12. In general, an e-mail that is sent to a 1&1 Mail subscriber is stored in the subscriber's "mail box" on 1&1 Mail servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on a 1&1 Mail server indefinitely.
13. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to 1&1 Mail's servers, and then transmitted to its end destination. 1&1 Mail often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the 1&1 Mail server, the e-mail can remain on a 1&1 Mail server indefinitely.
14. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by 1&1 Mail but may not include all of these categories of data.
15. A 1&1 Mail subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by 1&1 Mail.
16. Subscribers to 1&1 Mail might not store on their home computers copies of the e-mails stored in their 1&1 Mail account. This is particularly true when they access their 1&1 Mail account through the web, or if they do not wish to maintain particular e-mails or files in their residence.
17. In general, e-mail providers like 1&1 Mail ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

18. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via 1&1 Mail's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.
19. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.
20. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

IV. RELEVANT FEDERAL OFFENSES

21. Based upon the information above, your affiant believes that there is probable cause to believe that on the computer systems owned, maintained, and operated by 1&1 Mail, as described above, there exists evidence, fruits, and/or instrumentalities of violations of Title 18 United States Code, Section 1343 - Wire Fraud and Section 1344 - Bank Fraud, allowing agents to seize records and other information (including content of communications) stored on servers being maintained by 1&1 Mail for the account and files associated with the e-mail account: **max.ring@lawyer.com**.


V. LEGAL AUTHORITY AND INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. If issued, I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require 1&1 Mail to disclose to the government copies of the records and other information (including the content of communications) located at the premises described in Attachment A ("Place to Be Searched") and particularly described in Attachment B, Part I ("Information to Be Disclosed by 1&1 Mail"). Upon receipt of the information described in Part I of Attachment B, government-authorized persons will review that information to locate the items described in Part II of Attachment B ("Information to Be Seized by the Government").

23. The government may obtain internet and e-mail content and subscriber information from a third party by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A). Any court with jurisdiction over the offense under investigation may issue a § 2703 warrant, regardless of the location of the server where information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike Rule 41 search warrants, a § 2703 warrant does not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).
24. If the government obtains a search warrant, there is no requirement that the third party give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), (c)(3).

VI. CONCLUSION

25. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that unknown targets have committed fraud in violation of 18 U.S.C. § 1344 and 1343. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that computer systems owned or operated by or in the control of 1&1 Mail, headquartered at 701 Lee Road, Suite 300, Chesterbrook, PA 19087, contain evidence, fruits, and instrumentalities of the crimes identified above. Accordingly, I request that the Court issue a search warrant.
26. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).


Special Agent Matthew K. O'Neill
United States Secret Service

Subscribed and sworn to before me
this 10th day of January, 2014


United States District Court Judge

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with the e-mail account **max.ring@lawyer.com**, that is stored at premises owned, maintained, controlled, or operated by 1&1 Mail, Inc., an e-mail provider headquartered at 701 Lee Road, Suite 300, Chesterbrook, PA 19087.

LBM
1-10-14
m/c

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by 1&1 Mail

To the extent that the information described in Attachment A is within the possession, custody, or control of 1&1 Mail, 1&1 Mail is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account(s), including copies of e-mails sent to and from the account(s), draft e-mails, the source and destination addresses associated with each e-mail; the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the types of service utilized, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account(s) status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between 1&1 Mail, Inc. and any person regarding the account(s), including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and/or instrumentalities of violations of wire fraud (18 U.S.C. § 1343) and banks fraud (18 U.S.C. § 1344), including, for the account(s) or identifier(s) listed on Attachment A, information relating to the following matters:

1. Correspondence with any employees at Besi.
2. Records and data relating to Besi.
3. Records and data relating to banks located in Hong Kong, China, ~~and Japan~~ *LBM 1-10-14*
4. Records and data relating to communications with other e-mail accounts or instant message accounts (including, but not limited to, Messenger accounts) regarding any of the above.
5. Records and data relating to who used, created, or communicated with the account(s) or identifier(s), including records about their identities and whereabouts.
6. Records and data relating to the use, or attempted use, of personal identifying information to establish bank accounts or effect bank transactions.